Jurnal Teknik Informatika (JUTIF)
Vol. 4, No. 1, Februari 2023, hlm. 85-95

DOI: https://doi.org/10.20884/1.jutif.2023.4.1.753
p-ISSN: 2723-3863
e-ISSN: 2723-3871

THE ROLE OF BLOCKCHAIN TO SOLVE PROBLEMS OF DIGITAL RIGHT MANAGEMENT (DRM)

Jehan Afwazi Ahmad[*1], Teduh Dirgahayu[2]

[1,2]Jurusan Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia, Indonesia
Email: [1]jehan.afwazi@gmail.com, [2]teduh.dirgahayu@uii.ac.id

(Naskah masuk: 13 Desember 2022, Revisi : 26 Desember 2022, diterbitkan: 10 Februari 2023)

Abstract

In recent years, internet user was grown significantly. Even though many problems arise due to internet abuse. The sectors affected by the internet is digital assets or digital right. Various ways are done to solve the violation. One of that ways is to develop digital protection or Digital Right Management (DRM). However, the DRM technology has several disadvantages such as there is no way to track the leak and prove a copyright violation, the user is unable to authenticate the content since the content source is unknown, there is no user restriction to download the content, the system isn't provided the feature to alienate ore transfer ownership the content to other, and the system using centralize model that requires many issues, especially trust issue. Fortunately, the blockchain is a decentralized, secure, reliable, immutable, and tamper-proof paradigm. The blockchain is also built upon public key cryptography and has a smart contract that can solve or complement DRM problems. This paper discusses how the blockchain solves DRM problems. The results show that blockchain solves DRM problems. A narrative literature review was conducted with several stages, including a source search of papers, articles and news articles on digital rights management and blockchain in the last five years. The next step is to identify keywords related to the topic, to review the sources, and to compile the paper.

Keywords: *Blockchain, Decentralization, Digital Copyright, DRM.*

PERANAN BLOCKCHAIN UNTUK MENGATASI KEKURANGAN TEKNOLOGI PENGELOLA HAK CIPTA DIGITAL (DRM)

Abstrak

Penguna internet dari tahun ke tahun terus mengalami peningkatan yang signifikan. Padahal terdapat banyak masalah yang timbul oleh karena penyalahgunaan internet. Salah satunya adalah masalah perlindungan hak cipta digital. Berbagai cara dilakukan untuk menekan pelanggaran ini. Salah satunya adalah dengan perlindungan melalui teknologi pengelola hak kekayaan intelektual (*Digital Right Management*, DRM). Namun, teknologi DRM nyatanya memiliki banyak kekurangan seperti sistem tidak mampu melacak kebocoran data dan membuktikan pelanggaran, tidak dapat meng-autentikasi konten ketika sumber informasi kontennya tidak lagi diketahui, baik karena konten tersebut telah rusak atau telah dimanipulasi, sistem tidak dapat memberikan batasan unduh bagi pengguna terhadap konten digital, sistem tidak dapat memindahkan hak kepemilikan suatu karya cipta kepada orang lain, dan sistem yang ada bersifat sentralisasi. Untungnya blockchain adalah sebuah teknologi yang mengusung sistem terdesentralisasi, bersifat immutable, dan aman yang memungkinkan menjadi solusi permasalahan sistem DRM yang ada. Makalah ini akan membahas bagaimana blockchain dapat menyelesaikan atau melengkapi kekurangan dari sistem DRM. Hasil makalah ini menunjukkan bahwa dengan beberapa sifat dan fitur blockchain seperti terdesentralisasi, *immutable*, *tamper-proof*, berjalan di atas kriptografi kunci publik, serta dukungan *smart contract* kekurangan sistem DRM dapat teratasi. Makalah ini disusun menggunakan narative literatur review dengan beberapa tahapan antara lain melakukan pencarian sumber berupa makalah, artikel dan berita dengan topik *digital right management* dan blockchain dalam kurun waktu lima tahun terakhir. Kemudian, identifikasi kata kunci yang berkaitan dengan topik, selanjutnya melakukan review sumber dan tahap terakhir adalah menyusun makalah.

Kata kunci: *Blockchain, Desentralisasi, DRM, Hak Cipta, Hak Kekayaan Intelektual.*

1. PENDAHULUAN

Dalam beberapa tahun terakhir, jumlah pengguna konten digital khususnya di Indonesia

meningkat secara signifikan. Hal ini tidak luput dari peran teknologi internet sebagai fasilitas komunikasi dan berbagi informasi bagi masyarakat. Menurut laporan yang dirilis oleh [1], saat ini jumlah pengguna internet telah mencapai 77 persen dari total penduduk Indonesia. Efek pandemi covid19 menjadi salah satu faktor utama meningkatnya penggunaan internet. Hal ini karena di masa pandemi, internet menjadi sarana utama bagi masyarakat untuk belajar dan bekerja. Pada awalnya pengguna internet berkisar 175 juta jiwa. Namun, setelah pandemi pengguna internet mencapai 210 juta jiwa. Pengguna internet ini akan terus berkembang seiring pembaruan inovasi yang memberikan banyak alternatif pendukung aktivitas kehidupan masyarakat. Di samping berbagai manfaat yang dirasakan, penggunaan internet juga menimbulkan berbagai masalah, salah satunya adalah masalah pelanggaran hak cipta digital. Hal ini karena syarat kerugian materi yang cukup besar [2]. Hak cipta merupakan bagian dari Hak Kekayaan Intelektual (HKI) yang menjadi dasar perlindungan hukum terhadap karya-karya hasil kemampuan intelektual manusia [3].

Berkenaan dengan masalah ini, banyak pegiat hak cipta dan pakar teknologi berupaya membuat teknologi pengelolaan hak cipta (*Digital Right Management*, DRM) untuk melindungi hak cipta digital secara efektif dan efisien. DRM merupakan sebuah sistem keamanan yang memiliki mekanisme tertentu untuk melindungi suatu aset digital yang bernilai (karya cipta) [4]. Mekanisme perlindungan yang diterapkan oleh DRM umumnya menggunakan *watermark*, enkripsi, *safe container*, *mobile agent*, dan sebagainya. Selain itu, DRM juga dapat mengontrol distribusi serta penggunaan karya digital tersebut. Karya cipta digital yang dilindungi dapat berupa konten/barang elektronik dalam media digital berbasis internet seperti karya musik, sinematografi, buku, perangkat lunak, dan sebagainya [3]. Tujuan diterapkannya DRM [5], yaitu: (i) Untuk melindungi konten digital, (ii) Menjamin keamanan distribusi, (iii) Memastikan originalitas konten, (iv) Menyediakan transaksi non repudiation (prinsip tak terbantahkan), (v) Mendukung identifikasi pencipta.

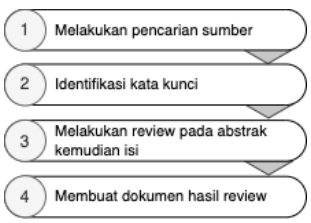
Menurut [6][7][8], teknologi DRM masih memiliki beberapa kekurangan, antara lain: (i) tidak mampu melacak kebocoran data dan membuktikan pelanggaran. (ii) tidak dapat meng-autentikasi konten ketika sumber informasi kontennya tidak lagi diketahui, baik karena konten tersebut telah rusak atau telah dimanipulasi, (iii) tidak dapat memberikan batasan unduh bagi pengguna terhadap konten digital, (iv) Tidak dapat memindahkan hak kepemilikan suatu karya cipta kepada orang lain, (v) bersifat sentralisasi, artinya penyimpanan konten diserahkan pada pihak ketiga. Hal ini memungkinkan peredaran hak cipta menjadi tidak transparan. Sebagaimana kebanyakan teknologi DRM yang beredar saat ini seperti Google Widevine Modular, Silverlight, Flash Air, Real Network, Windows DRM, serta Apple DRM hanya berfokus pada enkripsi konten digital dan manajemen lisensi sehingga beberapa poin yang menjadi tujuan penerapan DRM pun belum terpenuhi [9].

Dengan permasalahan tersebut, arsitektur DRM membutuhkan sebuah teknologi yang tepat untuk mencapai tujuan penerapan DRM yang diharapkan. Teknologi Blockchain menyediakan sebuah metode pencatatan transaksi sejenis buku besar terdesentralisasi dalam jaringan *peer-to-peer* (P2P) dengan melibatkan banyak partisipan untuk memverifikasi setiap transaksi yang dibuat. Setiap transaksi yang selesai dibuat akan disimpan ke dalam sebuah *block* yang berurutan secara kronologis dengan struktur dan mekanisme komputasi yang sulit untuk diubah. Dalam blockchain, setiap partisipan diizinkan untuk melacak transaksi yang terjadi tanpa perlu adanya pihak ketiga [10][11]. Dengan mekanisme seperti itu, memungkinkan setiap transaksi akan tercatat secara transparan sehingga menjamin keamanan distribusi, memastikan sumber informasi konten dapat di-autentikasi, dan pelanggaran serta membuktikan pelanggaran yang terjadi dapat dilacak. Disisi lain, agar dapat melakukan pencatatan kepemilikan dan pemindahan hak kepemilikan sebuah konten dapat menggunakan teknologi *smart contract. Smart Contract* adalah sebuah fitur atau program yang berjalan dalam jaringan blockchain yang memungkinkan pengaturan kontrak antara dua pihak secara otomatis di dalam blockchain. Dengan pemaparan terebut, makalah ini akan mengulas mengenai bagaimana teknologi blockchain menjadi solusi untuk mengatasi kekurangan sistem DRM saat ini. Pembahasan makalah ini akan memberikan contoh implementasi sistem DRM dengan blockchain pada transaksi buku digital.

2. METODE PENELITIAN

Narrative Literature Review adalah salah satu jenis literatur review yang akan mengulas dan menarik kesimpulan dari sekumpulan literatur pada sebuah topik tertentu [12]. Tujuan dari metode ini adalah untuk mengidentifikasi beberapa penelitian yang menggambarkan suatu topik tertentu. Metode ini tidak memiliki tahapan sistematis atau standar tertentu, tetapi setidaknya memuat ulasan kritis dari sebuah paper tertentu [13].

Atas dasar penjelasan tersebut, metode *Narrative Literature Review* untuk menyelesaikan penulisan makalah. Tahapan yang dilakukan dalam menyusen makalah ini ditunjukkan pada Gambar1.



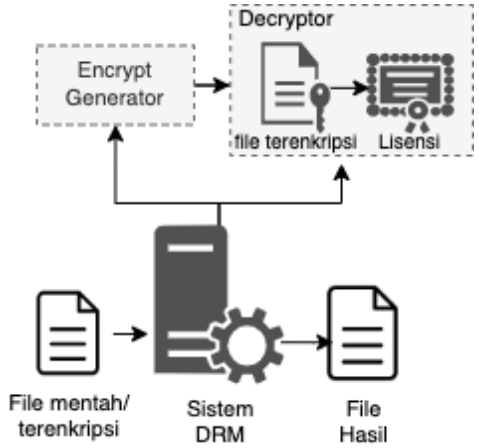
Gambar1 Tahap penyusunan Makalah

Penyusunan makalah ini akan dimulai dengan melakukan pencarian sumber dengan topik Digital Right Management and Blockchain pada lima tahun terakhir (2017 s/d 2022). Namun, beberapa sumber tambahan pada tahun sebelumnya dipertimbangkan untuk menjadi acuan juga. Sumber topik yang dicari berupa makalah, buku, berita, atau artikel. Selanjutnya menetukan kata kunci berupa blockchain, *digital right management*, drm, drmchain, teknologi pengaman digital, *content protection*, hak cipta digital, enkripsi, *smart contract*. Tahap selanjutnya, dilakukan review pada beberapa sumber yang didapatkan. Pada tahap terakhir dilakukan pembuatan dokumen hasil review.

3. HASIL DAN PEMBAHASAN

3.1. Digital Right Management

DRM merupakan teknologi pengamanan digital yang digunakan untuk melindungi aset digital (karya cipta) dengan cara mengontrol distribusi serta penggunaan aset digital [4]. DRM adalah sekumpulan sistem yang melindungi hak cipta berupa konten digital, seperti dokumen, musik, video dan konten elektronik yang tersimpan dan dapat dipindahkan melalui media elektronik [5]. DRM merupakan kombinasi dari teknologi, hukum dan kebijakan hak cipta serta model bisnis yang dibuat untuk mengontrol pendistribusian HKI. Tujuan penerapan DRM adalah memberikan perlindungan konten digital, memastikan keaslian konten, menyediakan transaksi non *repudiation* (tak terbantahkan) dan mendukung proses identifikasi sumber konten. Secara sederhana arsitektur sistem DRM ditunjukkan pada 2.



Gambar 21 Arsitektur Sistem DRM

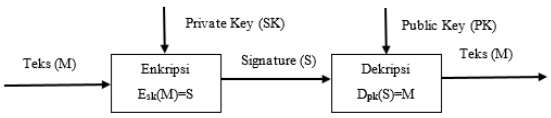
Terdapat dua proses dalam arsitektur sistem DRM, yaitu proses enkripsi file dan dekripsi file. Pada proses enkripsi, masukan berupa file mentah yang kemudian diolah pada mesin *encrypt generator* yang menghasilkan file terenkripsi dan lisensi. File terenkripsi adalah file yang sudah dienkripsi dengan kunci tertentu, sedang file lisensi adalah file yang berisi informasi yang umumnya berupa metadata, kunci, dan aturan hak akses dari file yang dilisensi. Pada proses dekripsi, masukan berupa file terenkripsi dan lisensi yang selanjutnya diproses pada mesin *decryptor* dan menghasilkan file yang diharapkan. Pada praktiknya, implementasi arsitektur sistem DRM ini dapat dilakukan dengan cara yang berbeda-beda, tapi konsep mekanismenya pada umumnya tetap sama.

Berdasarkan fungsinya, sistem DRM terbagi menjadi 3 bagian [14], yaitu: (i) DRM *manager* yang bertugas sebagai melakukan validasi dan dekripsi konten, (ii) DRM *security* bertugas untuk menangani proses kriptografi pada konten, (iii) aplikasi DRM yang bertugas untuk menjalankan (*rendering*) konten. Dalam hukum perlindungan teknologi, DRM atau bisa disebut juga *Technologies Protection Measure* (TPM) memiliki beberapa metode untuk melakukan kontrol dan menjaga keamanan data [5].

1. *Encryption*

Encryption adalah suatu algoritma kriptografi untuk mengkodekan suatu konten dengan sebuah sandi. Algoritma ini secara umum akan mengacak data sehingga menjaga kerahasian sebuah data/pesan. Lawan dari *Encryption* adalah *Decryption* yang merupakan proses kebalikan dari proses *encryption* yang akan mengembalikan data terenkripsi menjadi data asli.

Selain teknik enkripsi yang telah dijelaskan, terdapat pula teknik enkripsi dengan menggunakan sepasang kunci *public* (PK) dan *private* (SC) untuk melakukan kriptografi yang biasa disebut kriptografi kunci publik. PK dan SC memiliki korespondensi yang sama, sehingga sebuah pesan yang dienkripsi dengan SC dapat didekripsi dengan PK. Dengan metode ini selain dapat menjaga kerahasiaan sebuah pesan, juga dapat digunakan untuk mengotorisasi pesan serta memastikan bahwa pesan tersebut tidak dapat disangkal oleh pengirim maupun penerima (*non-repundation*). Secara teknis, proses kriptografi public key dan private key ditunjukan pada 3.



Gambar 3 Proses Kriptografi Kunci Publik

Sebuah pesan akan dienkripsi oleh pengirim pesan menggunakan SC, kemudian pesan tersebut akan diteruskan kepada penerima pesan. Penerima pesan dapat membuka pesan tersebut jika hanya pengirim pesan memberikan PK kepada penerima pesan. Dengan cara tersebut, maka seorang pengirim pesan tidak akan bisa menyangkal bahwa dia benar-benar mengirim pesan.

2. *Watermark*

Watermark adalah proses menyisipkan atau menempatkan sebuah informasi ke dalam sebuah data

baik berupa dokumen, gambar, musik atau video yang berisi informasi tertentu tanpa mengubah kualitas dari konten. Terdapat beberapa syarat umum untuk melakukan teknik *watermarking*, antara lain [15]:

- *Imperceptible*, *watermark* yang disisipkan tidak bisa dideteksi panca indra manusia
- *Robustness*, *watermark* yang disispuan tahan dari kerusakan baik karena proses *editing* atau manipulasi serta tidak mudah untuk di ekstrak
- *Secure*, *watermark* yang disisipkan seharusnya tidak mudah diekstrak, dihilangkan, atau dirusak.

Kategori *watermarking* jika dilihat dari kenampakan secara kasat mata terbagi menjadi dua hal, yaitu *visible watermarking* dan *invisible watermarking.*

- *Visible watermarking*

Pada kategori ini memungkinkan panca indra dapat melihat *watermark* pada sebuah dokumen. Hal ini sengaja ditampakan karena alasan tertentu. Dengan begitu *watermark* ini tidak memenuhi syarat *imperceptible*. *Watermark* jenis ini memiliki kelemahan yaitu mudah dihapus karena kebanyakan memiliki kontras yang berbeda yang di beri *watermark*, sehingga tidak memenuhi syarat *secure*. Namun, *watermark* jenis ini memenuhi syarat *robusness*, karena memiliki ketahanan yang bagus.

- *Invisible watermarking*

Kebalikan dengan *visible watermarking*, *watermark* jenis ini tidak dapat dilihat oleh panca indra. *Watermark* jenis ini lebih sulit dibuat, karena harus mempertahankan kualitas dokumen dan harus mempertimbangakn persyarayan *imperceptible*, *secure* dan *robusness. Watermark* jenis ini memiliki ketahanan yang kurang bagus.

Dari penjelasan mengenai sistem DRM diketahui bahwa komponen yang bekerja pada sistem DRM hanya dapat digunakan untuk melindungi konten digital dengan proses enkripsi untuk kepentingan autentikasi dan pemberian watermark untuk melacak dan membuktikan keaslian [9]. Melacak dan membuktikan keaslian ini dapat dilakukan secara manual dengan melihat tanda lisensinya (*watermark*) atau meng-autentikasi melalui sistem DRM. Namun, ketika konten tersebut telah dimanipulasi baik dengan cara merusak atau menghilangkan tanda lisensinya, maka sistem DRM tidak lagi berfungsi karena sumber konten tidak dapat dikenali atau di-autentikasi. Dengan begitu, penyebaran konten menjadi susah dikendalikan [6]. Peran *non-repundiation* yang diterapkan pada sistem DRM ini masih dilakukan oleh perantara (arbitrase) atau dapat juga dilakukan dengan mekanisme kriptografi kunci publik jika hanya mekanisme tersebut diterapkan. Disamping itu, teknologi DRM yang beredar saat ini hanya berfokus pada enkripsi konten dan managemen lisensi, sehingga tidak ada cara untuk memeriksa dan melacak pelaku pelanggaran [9]. Selain itu, fasilitas untuk memindahkan hak kepemilikan baik dengan meminjamkan, memberikan, atau menjual konten tidak dapat dilakukan dengan sistem DRM yang ada, padahal hal tersebut merupakan hal yang penting [7]. Disamping hal tersebut, sistem DRM yang ada saat ini umumnya diterapkan pada sistem terpusat yang mensyaratkan informasi data dan transaksi tidak transparan dan terdapat kemungkinan terjadi kerusakan pusat sistem baik karena kegagalan sistem ataupun serangan *cyber* [8].

3.2. Blockchain

Blockchain merupakan sebuah teknologi yang memiliki paradigma terdesentralisasi/tersebar. Paradigma ini merupakan kebalikan dari model sistem sentralisasi/terpusat. Pada model sistem sentralisasi, data pengguna akan diserahkan sepenuhnya kepada pihak penyedia layanan dan diletakkkan pada pusat sistem [8]. Dengan mekanisme tersebut, tidak ada jaminan privasi dan keamanan data yang tersimpan. Apabila terjadi kegagalan pada sistem, akan berdampak pada keseluruhan sistem yang mungkin mengakibatkan kerusakan atau kehilangan data. Selain itu, tidak ada kepastian bahwa pihak penyedia layanan benar-benar memegang komitmen untuk tidak membocorkan data. Sedangkan kontrak perjanjian antara pengguna dan penyedia layanan hanya sebatas persetujuan, sehingga penyelesaian sengketa umumnya sulit dilakukan. Dengan begitu, sistem dengan model setralisasi ini memiliki masalah utama yaitu masalah kepercayaan (*trust issue*). Adanya *trust issue* tersebut, sistem terdesentralisasi dapat menjadi solusi yang tepat.

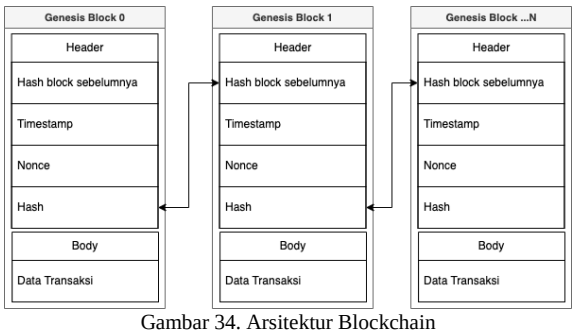
Dalam hal ini, salah satu kasus yang dapat dijadikan contoh sederhana untuk menjelaskan sistem terdesentralisasi adalah konsep pinjam meminjam buku [16]. Misalnya terdapat tiga orang yang memiliki sejumlah buku. Mereka akan saling berbagi bukunya dengan menjaga rekam jejak transaksi peminjaman buku agar tidak saling tertukar. Jika menerapkan konsep sentralisasi, maka ditunjuk satu orang yang terlibat dalam transaksi tersebut untuk mencatat setiap pertukaran/transaksi buku. Namun, bagaimana jika pencatat transaksi tersebut suka mencuri buku. Dengan begitu, akan timbul ketidakpercayaan terhadap pemegang catatan. Karena sangat mungkin bagi pemegang catatan untuk memanipulasi catatannya.

Jika menerapkan konsep terdesentralisasi pada kasus ini, maka ketiga orang tersebut akan saling memegang catatan dan mencatat setiap pertukaran/transaksi yang terjadi. Misalnya pihak pertama meminjamkan bukunya ke pihak kedua. Setelah transaksi terjadi, pihak pertama akan mengumumkan kepada semua peserta pinjam meminjam dengan menyatakan bahwa dia telah meminjamkan bukunya ke pihak kedua. Setelah diumumkan setiap peserta akan memastikan dengan melihat bahwa pihak kedua memiliki buku yang dipinjamkan pihak pertama. Setelah itu memastikan

hal itu, semua peserta akan menyepakati kemudian mencatat transaksi tersebut di buku catatan masing-masing dengan menyisipkan sebuah segel berupa tanda atau nomor yang disepakati bersama. Mekanisme kesepakatan menyegel catatan transaksi dengan sebuah tanda/nomer tertentu tersebut diumpamakan dengan mekanisme konsensus.

Dengan cara tersebut, apabila terdapat salah satu orang mungubah catatan, maka sulit baginya untuk mempertahankan kecurangannya karena masing-masing peserta memegang catatan dengan segel yang sama, sehingga apabila terdapat perbedaan, maka dipastikan terdapat kecurangan. Selanjutnya, bagaimana jika dua orang berkonspirasi untuk bertindak curang mengubah catatan. Dalam sistem terdesentralisasi yang mengusung konsep konsensus, kecurangan seperti itu mungkin dapat terjadi karena mayoritas pemegang catatan/partisipan (>50%) yang memiliki data yang sama dianggap valid [17]. Namun, kenyataannya proses validasi tidak hanya melibatkan tiga atau beberapa partisipan saja. Jumlah partisipan yang terlibat dalam proses validasi bisa jadi sangat banyak, bahkan termasuk pihak yang tidak terlibat secara langsung dalam transaksi tersebut. Oleh karena itu sulit bagi seseorang untuk berkonspirasi mendapatkan konsensus lebih dari 50% peserta.

Dalam blockchain, mekanisme konsensus atau kesepakatan bersama untuk menambahkan *block* kedalam *blockchain* diwakili oleh node. Node merupakan sebuah komputer yang terhubung dengan jaringan blockchain [18]. Node tersebut akan berkomunikasi dan saling berbagi informasi dengan komputer lain yang terhubung. Peran utama node adalah menyebarkan dan memvalidasi transaksi, menyimpan riwayat transaksi blockchain, dan menjaga konsensus satu sama lain. Setiap transaksi yang selesai dibuat akan diterima oleh node kemudian disebarkan ke setiap node lain melalui jaringan *peer-to-peer* (P2P) [9]. Transaksi yang diterima oleh node, kemudian akan divalidasi dan disepakati sebelum dibuat menjadi *block* baru. Transaksi tersebut dianggap gagal apabila lebih dari 50% node yang berpartisi tidak menyepakatinya. Semakin banyak node yang berpartisipasi dan mengkonfirmasi transaksi, keamanan dan integritas data menjadi semakin kuat.



Gambar 34. Arsitektur Blockchain

Secara umum arsitektur blockchain ditunjukkan pada Gambar 34. Terdiri dari sejumlah block yang terkait satu dengan yang lain. Setiap blockchain memiliki *block* pertama yang disebut *genesis block* sebagai acuan referensi *block* setelahnya. Struktur *block* dalam blockchain terdiri dari *block header* dan *body*. *Block header* berguna untuk identifikasi *block* tertentu di dalam keseluruhan blockchain [16]. Komponen *block header* terdiri dari beberapa komponen antara lain:

- Hash block sebelumnya

  Merupakan sebuah kode unik yang digunakan digunakan untuk mereferensi *block* sebelumnya pada blockchain.
- Timestamp

  Nilai yang menunjukkan waktu ketika *block* ditambahkan ke blockchain.
- Nonce (*Number Use Only One*)

  Nilai atau nomor dari proses penambangan (*mining*) yang digunakan untuk mendapatkan hash *block* yang diterima.
- Hash

  Sebuah kode unik yang mengidentifikasi *block* pada blockchain.

Kode hash pada sebuah *block* dibuat melalui fungsi hash. Fungsi hash akan memetakan sejumlah data menjadi satu string karakter yang bersifat deterministik. *Block* hash hasil dari fungsi hash ini kemudian disimpan atau disematkan ke dalam *block* selanjutnya. Apabila data di dalam *block* sebelumnya diubah, maka hash dari *block* sebelumnya juga akan berubah sehingga *block* yang mengikutinya menjadi tidak valid atau terputus. Dengan mekanisme rumit seperti ini, data yang telah disematkan ke dalam blockchain sangat sulit untuk diubah [19]. Kemampuan seperti ini membuat blockchain disebut bersifat *immutable*. Kelebihan yang dihasilkan dari sifat ini adalah kemampuannya untuk mendeteksi gangguan yang menyebabkan kerusakan data (*Tamper-proof*). Sebagaaimana dijelaskan bahwa hash adalah sebuah kode unik yang diumpamakan sebagai rantai *block* di dalam blockchain. Apabila terdapat seseorang berusaha untuk mengubah data pada salah satu *block*, maka dia harus mengubah setiap hash pada *block* yang mengikutinya. Belum juga dia harus mengubahnya pada seluruh jaringan blockchain yang terhubung. Oleh karena itu, setiap gangguan yang dapat menyebabkan kerusakan menjadi mudah untuk dideteksi.

Dalam mencetak sebuah hash, fungsi hash memiliki beberapa karakteristik yaitu: (i) deterministik artinya sebuah data atau pesan yang sama akan selalu menghasilkan kode hash yang sama, (ii) proses searah artinya ketika sebuah pesan dienkripsi akan tidak dapat dikembalikan ke data semula, (iii) Perbedaan satu karakter pada sebuah pesan akan selalu menghasilkan kode hash yang berbeda sahingga kecil kemungkinan akan menghasilkan kode hash yang sama. Dengan cara ini,

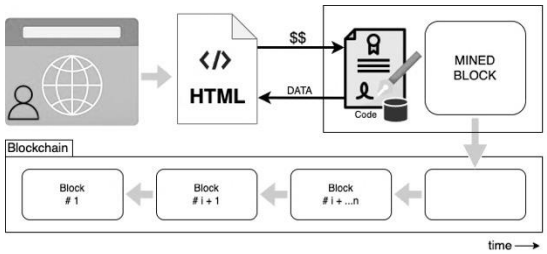
akan sulit membedakan antara kode hash yang satu dengan yang lain.

Salah satu proses di dalam kerja blockchain adalah proses mining (penembangan). Mining adalah sebuah proses komputasi matematis yang dilakukan oleh mesin (*miner*) untuk mendapatkan kode hash yang terverifikasi sesuai kriteria yang ditentukan. Sedangkan proses untuk mendapatkan kode hash dengan mekanisme konsensus dalam jaringan blockchain tersebut disebut *proof of work* (PoW) [20]. Proses penambangan dengan PoW membutuhkan perangkat daya dengan komputasi yang tinggi, semakin banyak perangkat yang digunakan untuk komputasi semakin besar pula peluang untuk mendapatkan hash sebagai *block* baru. Oleh karena PoW memiliki beberapa masalah terkait keamanan serta memakan konsumsi energi yang sangat besar, algoritma Proof-of-Stack (PoS) dibuat sebagai alternatif mekanisme konsensus yang dapat digunakan. Dengan mekanisme PoS penambang diharuskan mempertaruhkan sejumlah asset koin mereka agar dapat menjadi validator untuk menghasilkan *block baru.* Semakin besar jumlah koin yang dipertaruhkan, semakin besar peluang untuk menjadi validator. Apabila validator berhasil memvalidasi transaksi akan diberi imbalan berupa koin. Sebaliknya, jika validator tidak berhasil memvalidasi transaksi, koin yang dipertaruhkan akan dipotong dan validator tidak dapat menjadi validator untuk beberapa waktu tertentu.

3.2.1. Smart Contract

Smart Contract (SC) adalah sebuah program yang disimpan dalam blockchain yang secara otomatis dieksekusi ketika sebuah kondisi yang dintentukan terpenuhi dan terverifikasi [6]. Secara teknis SC menggunakan konsep "jika…maka" dalam mengeksekusi sebuah transaksi. Adanya SC menghilangkan proses tradisional yang mensyaratkan formalitas dengan birokrasi administrasi yang panjang tanpa mengurangi keaslian dan kredibilitas. Keuntungan dari SC ini yaitu: (i) mengurangi ketergantungan pada pihak ketiga (perantara), (ii) proses transaksi *realtime*, artinya transaksi yang dilakukan memiliki waktu yang singkat setelah kriteria terpenuhi, (iii) transparansi dan keamanan transaksi, oleh karena SC didasarkan pada blockchain yang menjamin data bersifat transparan dan *immutable*, memungkinkan kesepakatan yang dibuat dapat dilakukan tanpa perlu mengenal satu sama lain. Hal ini juga dapat menghindari terjadinya pelanggaran seperti manipulasi klausul kontrak atau kesalahan dalam pengelolaan dan pelaksaan kesepakatan.

Sebagaimana SC adalah sebuah program yang berarti sebuah kode yang disimpan, diverifikasi, dan dieksekusi di dalam platform blockchain. Selain itu code ini yang digunakan untuk mengeksekusi dan menyelesaikan sebuah ketentuan dalam kontrak kesepakatan. Meskipun SC dieksekusi secara otomatis oleh komputer, beberapa bagian SC menyaratkan masukan dari pengguna/manusia. Secara umum sistem *smart contract* ditunjukkan pada Gambar 5.



Gambar 5. Sistem Smart Contract

Smart contract memiliki saldo akun, penyimpanan personal, dan *excutable code* [21]. SC memiliki sebuah *state* mengacu pada keadaan transaksi, yang berarti pihak yang terlibat dalam transaksi akan mengalami perubahan. Misalnya, seseorang mengirimkan sejumlah uang ke rekening orang lain, maka akan terjadi perubahan pada kedua sisi orang tersebut. State kontrak terdiri dari penyimpanan personal dan saldo kontrak. *State* ini akan disimpan dalam salah satu *block* dan akan diperbarui setiap kali kontrak dipanggil. Setiap kontrak akan ditetapkan pada sebuah alamat 20 *bytes*. Setelah sebuah kontrak di-*deploy* dalam blockchain, kontrak tersebut tidak lagi dapat diubah. Untuk menjalankan sebuah kontrak, secara sederhana pengguna harus membuat sebuah transaksi kepada alamat kontrak. Transaksi ini kemudian dieksekusi oleh setiap node yang terlibat untuk kemudian divalidasi, demikian state kontrak juga akan diperbarui. SC dapat membaca dan menuliskan data ke dalam penyimpanan personal (*personal storage)*, menyimpan uang di dalam kontrak saldo, dan juga dapat membuat kontrak baru. Selain itu, dengan kemampuannya untuk identifikasi pengguna melalui sebuah alamat, SC juga dapat memberikan kontrol akses kepada pengguna.

Menurut [22] terdapat 4 fase yang terjadi dalam siklus *SC*:

1. Penciptaan (*Creation*)

Fase ini dibagi menjadi dua tahapan yaitu negosiasi dan implementasi. Tahap negosiasi akan dilakukan pertama kali bersama dengan para pihak terkait untuk menyepakati isi dan tujuan kontraknya. Pada tahap implementasi, kontrak yang telah disepakati tersebut diubang menjadi sebuah kode. Tahapan ini akan terus berulang sampai kesepakatan kontrak dan implementasi kode yang dibuat selesai. Hal ini dilakukan, karena ketika SC telah di-*deploy* di blockchain, kontrak tersebut tidak dapat diperbaharui.

2. Pembekuan (*Freeze*)

Fase ini dimulai setelah SC di-*deploy* ke dalam blockchain. Dalam fase ini SC bersifat publik sehingga para pihak yang terlibat dapat melakukan transaksi seperti pada umumnya. Transaksi SC dalam

blockchain menggunakan metode *escrow* yang memberlakukan penahanan pembayaran sampai seluruh klausul pada kontrak terpenuhi dan node berperan untuk memastikan semua prasyarat kontrak terpenuhi.

3. Pelaksanaan (*Execute*)

Setelah semua prasayarat terpenuhi, selanjutnya kontrak disimpan di dalam blockchain dan didistribusikan pada semua node. Setelah itu, kontrak akan divalidasi dan mesin penerjemah SC akan mengeksekusi kode. Eksekusi SC menghasilkan sebuah transaksi baru dan *state* baru. Hasil dari SC dan *state* selanjutnya diserahkan ke node blockchain yang selanjutnya dilakukan konsensus untuk menghasilkan *block* baru.

4. Finalisasi (*Finalize*)

Setelah SC dieksekusi, asset digital dipindahkan, dan semua transaksi telah dikonfirmasi, maka kontrak telah terpenuhi.

Selain itu, sistem kerja SC yang melibatkan blockchain dalam suatu transaksi terbagi menjadi dua [23]:

1. On-Chain

Merupakan transaksi SC yang terjadi di dalam blockchain. Transaksi ini sama halnya yang telah dijelaskan pada siklus SC. Berawal dari penciptaan, pembekuan, pelaksanaan, dan finalisasi. Artinya semua transaksi yang terjadi tidak melibatkan pihak diluar blockchain.

2. Off-Chain

Berbeda dengan transaksi *on-chain*, transaksi ini melibatkan pihak ketiga, seperti konversi uang crypto ke nilai rupiah, memberikan *watermark* pada sebuah dokumen, dan sebagainya. Hal ini umumnya dilakukan sebelum informasi tersebut digunakan oleh SC. Atau dapat pula informasi tersebut diverfikasi atau disaring melalui suatu perangkat yang disebut ”*oracle*” sebelum selanjutnya dinyatakan dapat memasuki blockchain dan digunakan oleh SC.

3.2.2. InterPlanetary File System (IPFS)

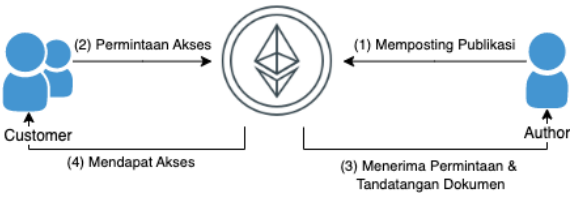
IPFS merupakan filesystem yang mengusung sistem terdesentralisasi yang terinsipirasi dari beberapa ide sukses penerapan sistem P2P seperti BitTorrent, Git, DHTs, dan SFS [24]. IPFS adalah salah satu teknologi pendukung blockchain yang secara spesifik menangani penyimpanan konten media dan referensi yang terdesentralisasi dan dikhususkan untuk blockchain Ethereum [25]. Konten yang dapat disimpan dan dibagikan pada IPFS ini antara lain, video, audio, dan teks dokumen. Sistem penyimpanan dan pendistribusian pada IPFS tidak tergantung pada satu node, melainkan disebarkan sejumlah node sehingga aplikasi menjadi lebih aman, cepat, tahan, handal, dan transparan. Response yang dikembalikan setelah mengunggah file ke IPFS berupa hash.

3.3. DRM Berbasis Blockchain

Ini merupakan contoh sub-bab kedua. Isinya dapat disesuaikan dengan kebutuhan

Dalam sistem DRM biasa berupa jual beli buku secara online (*ecommerce*) [26], terdapat tiga aktor yang terlibat dalam sistem *ecommerce*, yaitu: *author*, *customer*, dan *publisher*. *Author* awalnya akan memilih *publisher* yang akan menerbitkan buku digital. Setelah itu *author* melakukan perjanjian dengan *publisher* secara luring. Setelah perjanjian dibuat, *publisher* dapat menjual bukunya kepada *customer* secara langsung. Kemudian hasil penjualan, akan dibagikan kepada pihak *author* sesuai perjanjian. Berkenaan dengan jumlah buku yang dijual dan total pendapatan yang diterima, diserahkan sepenuhnya kepada pihak publisher. Mekanisme seperti itu, tentu kurang menjamin transparansi data transaksi yang dilakukan pihak *publisher* dan *customer*. Artinya segala informasi terkait buku yang disebarkan dan hasil yang diperoleh tidak diketahui sepenuhnya oleh *author*. Selain itu, data dan transaksi yang tersimpan berada di pusat sistem. Dengan mekanisme ini dimungkinkan apabila terjadi kegagalan pada pusat sistem akan berdampak pada sistem seluruhnya dan dimungkinkan juga terjadi kecurangan penyebaran data ilegal yang dilakukan oleh pihak ketiga sehingga isu kepercayaan timbul.

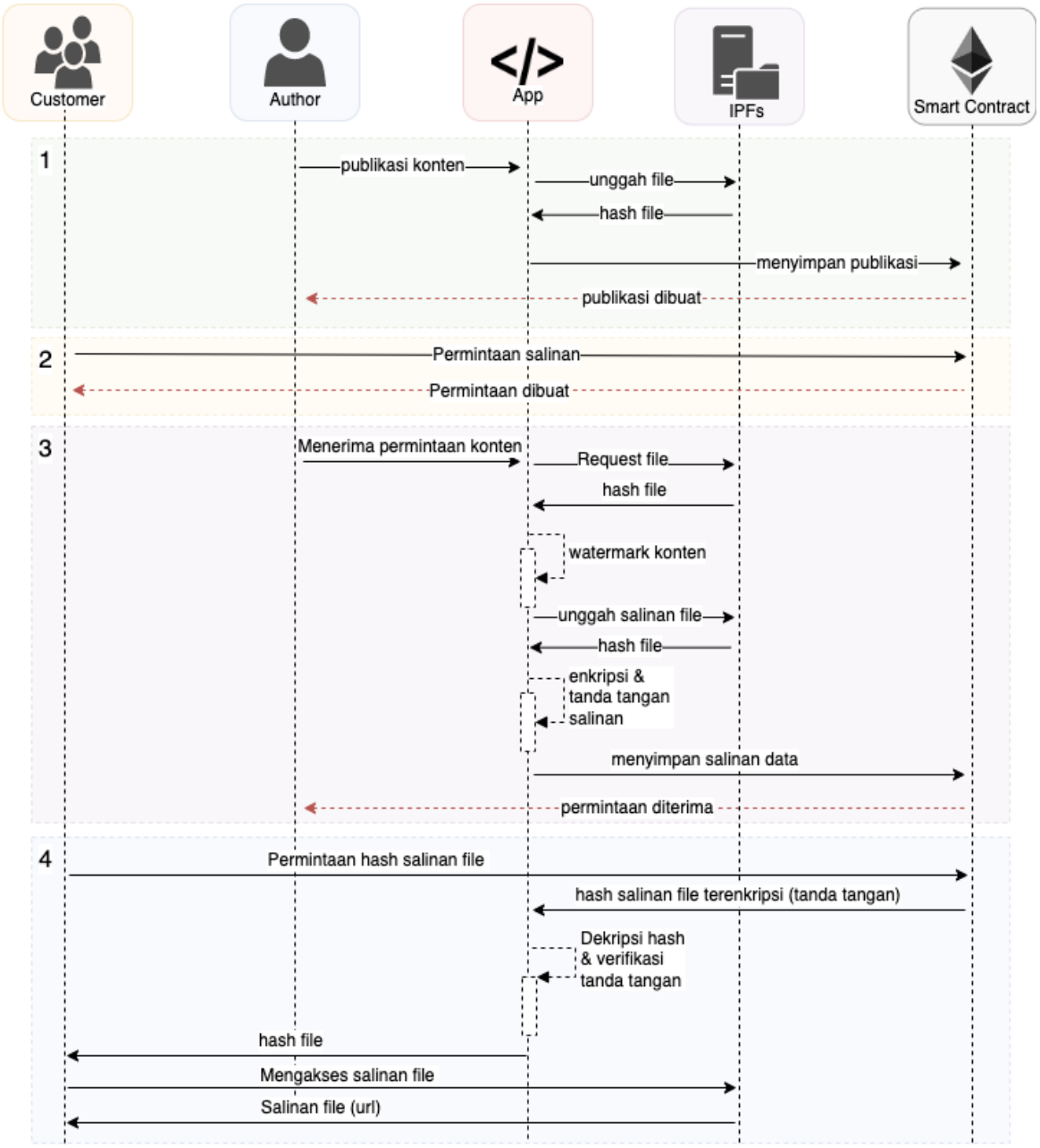
Dalam sistem DRM berbasis blockchain peran *publisher* sebagai perantara penjualan antara *author* dan *customer* akan ditangani secara otomatis oleh *SC* dan disimpan di dalam blockchain. Dengan mekanisme ini, setiap transaksi yang terjadi akan tercatat secara historis dan dapat dilihat oleh pihak yang terlibat secara transparan. Dalam hal ini semua pihak yang terlibat akan dapat mengetahui jumlah buku yang disebarkan dan pendapatan yang didapatkan. Gambar mengilustrasikan sistem DRM berbasis blockchain secara sederhana.



Gambar 6. Alur Penerbitan dan Pemberian Lisensi Sistem DRM Berbasis Blockchain

Dalam sistem DRM berbasis blockchain komponen utama DRM yang dimaksud pada Gambar 21. ditangani oleh smart contract. File utama yang diproteksi akan disimpan dalam file server (IPFS) dan mengembalikan nilai hash. Kemudian file tersebut disalin dan diberi *watermark* serta ditanda tangani *author*. Selanjutnya metadata dari file tersebut disimpan kembali ke dalam blockchain melalui smart contract. Setiap ada permintaan *customer* untuk mengakses file, sistem akan mengambil metadata yang tersimpan dalam blockchain dari SC kemudian memverifikasi tanda tangan. Data yang terverifikasi akan bisa jalankan oleh customer melalui aplikasi

Gambar 7 menunjukan diagram sequen yang menampilkan kesluruhan proses transaksi yang terjadi pada sistem DRM berbasis blockchain. Pada diagram tersebut terdiri dari 4 proses.



Gambar 7 Diagram Sequence Sistem DRM Berbasis Blockchain

1. Proses Publikasi

Author membuat (*publish*) sebuah konten baru berisi informasi terkait konten kemudian memilih file yang ingin diunggah. Selanjutnya, aplikasi akan mengunggah file yang dipilih tersebut ke IPFS. Kemudian IPFS akan menggembalikan nilai hash dari file yang diunggah. Hash tersebut selanjutnya disematkan ke dalam data dari konten yang akan dipublish. Setelah itu, aplikasi akan melakukan pemanggilan kepada SC untuk menyimpan informasi kontent tersebut ke dalam blockchain. Setelah informasi berhasil disimpan, SC akan memberikan notifikasi kepada *author* berupa status bahwa proses publikasi telah berhasil dibuat.

2. Proses Permintaan Salinan

Customer melakukan permintaan salinan konten yang dipublikasi oleh *author* kepada smart contract. Dengan mengirimkan data berupa identitas *customer* dan PK. Setelah itu, smart contract akan memberikan notifikasi kepada *author* berupa informasi bahwa terdapat permintaan salinan dan notifikasi kepada *customer* berupa status bahwa permintaan salinan telah berhasil dibuat.

3. Proses Penerimaan Salinan

Author akan memeriksa dan menerima permintaan salinan melalui aplikasi. Selanjutnya, aplikasi akan mengunduh file dari IPFS kemudian memberikan *watermark* kepada file kemudian menggunggah kembali ke IPFS. Selanjutnya, respon file yang diunggah ke IPFS berupa hash dienkripsi menggunakan PK dari *customer* dan ditandatangani oleh *author.* Setelah itu, data berisi hash file dan data *signature* yang terenkripsi dikirim ke SC untuk disimpan ke dalam blockchain.

4. Proses Mengakses Salinan

Customer melakukan permintaan pada SC untuk mengambil hash file salinan melalui aplikasi dengan mengirimkan SK. Setelah itu, SC memberikan respon berupa hash file yang terenkripsi. Selanjutnya, aplikasi akan mendekripsi data tersebut. Dekripsi akan menghasilkan hash data dan *signature* yang kemudian dilakukan proses verifikasi. Jika hasil verifikasi valid, maka hash file akan dikirimkan ke *customer* yang kemudian customer dapat dapat menggunakan hash file tersebut untuk mengakses file ke IPFS server.

4. DISKUSI

Berdasarkan tujuan diterapkannya sistem DRM [5] dan beberapa kelemahan sistem DRM yang diungkapkan oleh [6][7][8], serta dari hasil pembahasan terkait kelemahan sistem DRM, maka dikumpulkan beberapa poin yang menjadi permasalahan DRM dan blockchain menjadi solusi menyelesaikan permasalahan tersebut. Beberapa poin tersebut, antara lain:

1. Menjamin keamanan distribusi
2. Memastikan originalitas konten
3. Menyediakan transaksi non-repundiation
4. Mendukung identifikasi pencipta
5. Melacak kebocoran dan membuktikan pelanggaran
6. Memberi batasan unduh dan memindahkan hak kepemilikan

Pembahasan yang disajikan dari makalah ini menjelaskan mengenai sistem DRM berbasis blockchain yang meliputi beberapa komponen DRM yang berjalan pada sistem blockchain. Dalam melindungi konten digital dari pembajakan, sama halnya dengan sistem DRM biasa, sistem ini melakukan enkripsi dan menyematkan sebuah tanda (*watermark*) pada konten tersebut yang ditunjukkan pada Gambar dalam proses permintaan dan penerimaan salinan. Dengan enkripsi konten, konten menjadi tidak dapat dibuka tanpa di-dekripsi. Sedangkan dengan *watermark*, keaslian konten dapat dibuktikan dengan memastikan *watermark* yang disematkan, baik melalui sistem ataupun secara kasat mata jika *watermark* yang disematkan bersifat *visible*.

Pada sistem DRM biasa, apabila sebuah konten telah dimanipulasi dengan menghilangkan atau merusak enkripsi maupun watermark, maka sistem DRM tidak lagi dapat mengenali konten tersebut. Begitu juga dengan pelaku pembajakan juga tidak dapat dilacak, hal itu karena sistem DRM tidak merekam jejak pelaku yang bertransaksi di dalam sistem. Selain itu, sistem DRM yang berjalan umumnya bersifat sentralisasi sehingga tidak ada jaminan bahwa sistem tersebut dapat dipercaya. Sedangkan pada sistem DRM berbasis blockchain, sebagaimana pembahasan terkait blockchain, bahwa blockchain bersifat terdesentralisasi, sehingga permasalahan *trust issue* dalam sistem DRM yang ada saat ini teratasi [16]. Sistem terdesentralisasi memungkinkan tidak ada pihak ketiga (penyedia layanan) yang menjadi perantara transaksi. Segala keputusan dalam sistem dikendalikan oleh pengguna sistem. Setiap pengguna dalam sistem blockchain akan saling memvalidasi dan mengkonfirmasi pada setiap transaksi yang terjadi dengan algoritma konsensus. Setelah proses konsensus selesai dan transaksi yang dilakukan dianggap valid, transaksi tersebut disegel dengan sebuah hash dan menjadi *block* baru dalam blockchain. *Block* tersebut akan disimpan secara kronologis sesuai urutan block tersebut dibuat. Sedangkan hash akan menjadi rantai *block* karena setiap *block* pada blockchain akan mereferensi hash *block* sebelumnya. Apabila data pada sebuah *block* dimanupulasi, hash pada *block* tersebut akan berubah, begitu juga urutan *block* menjadi terpecah. Mekanisme seperti ini, tentu dapat menjamin keamanan distribusi, dapat memastikan keaslian data atau dokumen, serta dapat melacak transaksi atau pelanggaran yang terjadi.

Selain itu, Teknologi blockchain dibangun di atas kriptografi kunci publik sebagai protokol keamanan yang memastikan keamanan pertukaran data dalam jaringan. Aspek keamanan seperti ini sangat penting dalam jaringan P2P, karena node-node yang terlibat tidak saling mengenal dan percaya satu sama lain, sehingga perlu adanya sistem keamanan yang memastikan bahwa informasi yang dikirim atau diterima pihak yang bertransaksi tidak bocor atau dicuri oleh pihak lain. Sistem keamanan ini akan menjamin *non-repundiation* transaksi. Artinya tidak dapat disangkal bahwa sebuah transaksi yang dilakukan benar-benar dilakukan oleh pihak yang terlibat di dalam transaksi tersebut. Dengan begitu, sistem yang dibuat di atas blockchain pasti menyediakan transaksi *non-repundiation* dan pencipta dapat diidentifikasi.

Sebagaimana, pembahasan mengenai model sistem DRM berbasis blockchain yang dibangun melalui SC. SC mengidentifikasi kontrak atau pengguna dengan sebuah alamat 20 *bytes* sehingga alamat tersebut menjadi identitas yang unik. Dengan alamat tersebut SC dapat mengenali pihak-pihak yang terlibat dalam transaksi termasuk pemilik dari aset digital. Dengan begitu, SC dapat memindahkan hak kepemilikan dari pihak satu ke pihak lain. Proses publikasi yang ditunjukkan Gambar sejatinya terdapat proses pemindahan hak kepemilikan dari alamat kontrak ke alamat akun pengirim. Oleh karena secara *default* hak kepemilikan kontrak adalah alamat

kontrak yang di-*deploy* [27]. Selain itu, pembatasan akses dalam SC sangat mungkin dilakukan. Seperti halnya dalam proses mengakses salinan file pada Gambar , customer tidak dapat mengakses file bila mana permintaan akses file belum diterima oleh *author*. Dengan begitu, pemindahan hak kepemilikan dan pembatasan akses dalam sistem DRM berbasis blockchain dapat dilakukan.

Beberapa penelitian yang menjadi acuan dalah penyusunan makalah ini adalah [8][26]. Penelitian tersebut mengusulkan sebuah desain DRM berbasis blockchain yang berfokus pada jual beli konten digital. Dalam peneltian [8] sistem yang dibangun melibatkan dua aktor, yaitu: pemegang hak cipta (*owner*) dan *customer*. Dalam proses inisiasi konten yang akan diterbitkan, *owner* dapat mengatur harga dan hak akses terhadap konten yang diterbitkan. Setelah konten diterbitkan, *customer* dapat membeli konten tersebut dengan membayar sejumlah biaya dan mendapatkan hak penggunaan sesuai dengan aturan yang diatur sebelumnya. Berbeda dangan penelitian oleh [26], yang melibatkan tiga aktor di dalam sistem. yaitu: *author*, *publisher*, dan *customer*. Desain yang diusulkan berfokus pada pembagian royalti yang didapatkan dari profit penjualan konten kepada *publisher* dan *author*. Namun, dalam penelitian yang diusulkan proses perjanjian antara *author* pihak *publisher* masih dilakukan diluar kontrak, padahal semestinya SC dapat mengakomodir perjanjian tersebut. Selain itu, penelitian oleh [8] hanya dapat diaplikasikan pada satu user, sehingga hal ini menjadi peluang untuk penelian selanjutnya.

5. KESIMPULAN

Masalah utama diri sistem DRM biasa adalah (i) tidak ada jaminan keamanan distribusi, (ii) tidak dapat memastikan originalitas serta mendukung identifikasi pencipta konten jika sumber konten tidak diketahui, (iii) tidak menyediakan transaksi non-repundiation, (iv) tidak dapat melacak kebocoran dan membuktikan keaslian, serta (v) tidak dapat memberikan batasan akses dan hak kepemilikan suatu konten, (vi) selain itu sistem DRM biasa menganut sistem setralisasi yang memiliki banyak masalah.

Hasil ini menunjukkan, bahwa teknologi blockchain menjadi solusi untuk menyelesaikan masalah DRM biasa. Sebagaimana blockchain mengusung paradigma terdesentralisasi, *bersifat immutable, dan tamper-proof*. Selain itu SC sebagai program yang berjalan dalam blockchain dapat mengidentifikasi pengguna, memindahkan hak kepemilikan serta membatasi akses pada pengguna.

Sebagai hasil makalah ini, direkomendasikan sebuah sistem DRM berbasis blockchain yang mengapilkasikan sistem jual beli atau peminjaman antara pihak *author*, *customer*, dan *publisher* yang dapat dilakukan tanpa perlu adanya kontrak secara langsung dengan pihak terkait. Sistem juga dapat membagi royalti secara adil kepada author, serta dapat memindahkan hak kepemilikan atau memberikan hak penggunaan dengan membatasi akses terhadap konten yang dipinjam.

DAFTAR PUSTAKA

[1] I. R. Dewi, "Data Terbaru! Berapa Pengguna Internet Indonesia 2022?," *09 Juni 2022*, 2022. https://www.cnbcindonesia.com/tech/20220609153306-37-345740/data-terbaru-berapa-pengguna-internet-indonesia-2022 (accessed Nov. 25, 2022).

[2] "Liputan Humas," 2021. https://www.dgip.go.id/artikel/detail-artikel/upaya-djki-tingkatkan-ranking-di-indeks-inovasi-global-indonesia?kategori=liputan-humas (accessed Oct. 12, 2022).

[3] Kementrian Hukum Hak Asasi Manusia Tim, "Modul Kekayaan Intelektual Tingkat Dasar Bidang Hak Cipta (Edisi 2020)," *Kementrian Huk. Hak Asasi Mns. Tim*, 2020.

[4] Irawati, "DIGITAL RIGHT MANAGEMENTS (TEKNOLOGI PENGAMAN) DALAM PERLINDUNGAN TERHADAP HAK CIPTA DI ERA DIGITAL," 2019, Accessed: Dec. 04, 2021. [Online]. Available: https://ejournal2.undip.ac.id/index.php/dplr/article/view/5022

[5] K. M. Simatupang, "Tinjauan Yuridis Perlindungan Hak Cipta dalam Ranah Digital," *J. Ilm. Kebijak. Huk.*, vol. 15, no. 1, p. 67, Mar. 2021, doi: 10.30641/kebijakan.2021.v15.67-80.

[6] A. Garba *et al.*, "A digital rights management system based on a scalable blockchain," *Peer-to-Peer Netw. Appl.*, vol. 14, no. 5, pp. 2665–2680, Sep. 2021, doi: 10.1007/s12083-020-01023-z.

[7] B. Rosenblatt, "Can Blockchain Disrupt The E-Book Market? Two Startups Will Find Out," *Aug 18, 2018,08:27am*, 2018. https://www.forbes.com/sites/billrosenblatt/2018/08/18/can-blockchains-disrupt-the-e-book-market-two-startups-will-find-out/?sh=25593b65a0b6 (accessed Oct. 13, 2022).

[8] Z. Zhang and L. Zhao, "A design of digital rights management mechanism based on blockchain technology," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10974 LNCS, pp. 32–46, 2018, doi: 10.1007/978-3-319-94478-4_3.

[9] Z. Ma, M. Jiang, H. Gao, and Z. Wang, "Blockchain for digital rights management," *Futur. Gener. Comput. Syst.*, vol. 89, pp. 746–764, Dec. 2018, doi:

10.1016/j.future.2018.07.029.

[10] X. Fei, "BDRM : A Blockchain-based Digital Rights Management Platform with Fine-grained Usage Control," vol. 6, no. 2, pp. 54–63, 2019.

[11] M. Zhaofeng, H. Weihua, and G. Hongmin, "A new blockchain-based trusted DRM scheme for built-in content protection," *Eurasip J. Image Video Process.*, vol. 2018, no. 1, Dec. 2018, doi: 10.1186/s13640-018-0327-1.

[12] M. Y. Elkins, "Using PICO and the brief report to answer clinical questions," *Nursing (Lond).*, vol. 40, no. 4, pp. 59–60, 2010, doi: 10.1097/01.NURSE.0000369871.07714.39.

[13] C. C. Trial, I. Findings, and D. Findings, "Defining and Analyzing the Problem," pp. 27–39, 2019, doi: 10.1016/B978-0-12-814449-7.00003-X.

[14] R. Muslim Ijtihadie, H. T. Ciptaningtyas, and T. Zabo, "Perancangan Sistem dengan Konsep DRM (Manajemen Lisensi Digital) dalam Studi Kasus Penjualan Lagu secara Online."

[15] A. Saelan, I. T. Bandung, and J. G. Bandung, "Analisis Beberapa Teknik Watermarking dengan Domain Spasial pada Citra Digital," no. 13508029, 2011.

[16] W.-M. Lee, *Beginning Ethereum Smart Contracts Programming*. 2019. doi: 10.1007/978-1-4842-5086-0.

[17] "Consensus mechanisms | ethereum.org," *September 29, 2022*, 2022. https://ethereum.org/en/developers/docs/consensus-mechanisms/ (accessed Dec. 08, 2022).

[18] D. Rezkitha, "Understanding Node and Its Function in Blockchain - Pintu Academy," *December 15, 2021*, 2021. https://pintu.co.id/en/academy/post/what-is-node#what-are-nodes (accessed Nov. 29, 2022).

[19] V. Chingath and R. Babu, "Advantage Blockchain Technology for the Libraries Open access and Resource sharing View project," 2020. [Online]. Available: https://www.researchgate.net/publication/341725555

[20] E. Hamilton, "PoW vs PoS vs PoA: Which is Better Consensus Algorithm? | Tech Times," *24 August 2021*, 2021. https://www.techtimes.com/articles/264508/20210824/pow-vs-pos-vs-poa-which-is-better-consensus-algorithm.htm (accessed Nov. 28, 2022).

[21] M. Alharby and A. van Moorsel, "Blockchain Based Smart Contracts : A Systematic Mapping Study," pp. 125–140, 2017, doi: 10.5121/csit.2017.71011.

[22] C. Sillaber and B. Waltl, "Life Cycle of Smart Contracts in Blockchain Ecosystems," *Datenschutz und Datensicherheit - DuD*, vol. 41, no. 8, pp. 497–500, 2017, doi: 10.1007/s11623-017-0819-7.

[23] S. Oktaviani and M. Kenotariatan, "Implementasi Smart Contract Pada Teknologi Blockchain Dalam Kaitannya Dengan Notaris Sebagai Pejabat Umum," *J. Kertha Semaya*, vol. 9, no. 11, pp. 2205–2221, 2021, [Online]. Available: https://doi.org/10.24843/KS.2021.v09.i11.p18

[24] J. Benet, "IPFS - Content Addressed, Versioned, P2P File System," no. Draft 3, 2014, [Online]. Available: http://arxiv.org/abs/1407.3561

[25] "Apa Itu IPFS Dan Kegunaannya Di NFT Project - Diginews.id," *April 1, 2022*, 2022. https://diginews.id/apa-itu-ipfs-dan-kegunaannya-di-nft-project/ (accessed Nov. 10, 2022).

[26] N. Nizamuddin, H. Hasan, K. Salah, and R. Iqbal, "Blockchain-Based Framework for Protecting Author Royalty of Digital Assets," *Arab. J. Sci. Eng.*, vol. 44, no. 4, pp. 3849–3866, Apr. 2019, doi: 10.1007/s13369-018-03715-4.

[27] "Access Control - OpenZeppelin Docs." https://docs.openzeppelin.com/contracts/3.x/access-control (accessed Dec. 09, 2022)..